

Notice of Allowability

Application No.

10/621,731

Examiner

Minh Dinh

Applicant(s)

PATRICK, KYLE NATHAN

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to examiner's amendment authorized on 10/05/07.
2. ☒ The allowed claim(s) is/are 22.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☒ All b) ☐ Some* c) ☐ None of the:
 1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Jack Friedman on 10/05/07.

The claims have been amended as follows:

1-4 (Canceled)

22 (New). A method of securely comparing a first document in possession of a first party and a second document in possession of a second party, without revealing the contents of the first document to the second party or the contents of the second document to the first party, said method comprising the steps of:

- i) said first and second parties each generating its own set of random data;
- ii) each party exchanging said set of random data and a shared hash function with the other party;
- iii) each party computing a first value consisting of the output of said shared hash function where the input to the hash function is the consecutive concatenation of the document in each said party's possession, followed by that party's set of random data, followed by the other party's set of random data;
- iv) each party computing a second value consisting of the output of said shared hash

Art Unit: 2132

function where the input to the hash function is the consecutive concatenation of the document in each said party's possession, followed by the other party's set of random data, followed by that party's set of random data;

v) each party sending its first value to the other party and receiving the other party's first value;

vi) each party comparing said other party's first value to its second value;

vii) each party concluding that if the said values are the same, then the two documents are the same, but that otherwise said two documents are different;

viii) after computing said first and second values according to steps iii) and iv) above, each said first and second parties sending confirmation to the other party that each said party's first and second values have been computed, and waiting for said confirmation from said other party that each said party's first and second values have been computed before proceeding;

ix) after one party has sent its first value to the other party according to step v) above, aborting the comparison if the other party does not respond with its first value within a pre-determined length of time;

x) after step i) and before step ii), each party examining the other party's set of random data for suitability and aborting the comparison if suitability is not established,

wherein said other party's random data is determined to be unsuitable if it is identical to said examining party's set of random data.

2. The following is an examiner's statement of reasons for allowance.

The present invention is directed to a method of comparing a document possessed by a first party and a second party without either party revealing the contents of the document to the other party, wherein each party (i) generates a first hash value from the document in that party's possession, random data generated by that party, and random data generated by the other party (in that particular order); (ii) generates a second hash value from the document in that party's possession, the random data generated by the other party, and the random data generated by that party (in that particular order); (iii) sends the first hash value to the other party and receives the other party's first hash value; (iv) and compares the received first hash value with the generated second hash value. More specifically, independent claim 22 identifies the uniquely distinct features: each party sends the first hash value to the other party only after it has sent a confirmation to the other party and receives a confirmation from the other party that the respective party has generated the first and second hash values. The closest prior art, Menezes et al. ("Handbook of Applied Cryptography"), discloses a method for comparing a document (i.e., a shared secret key) possessed by two parties, A and B, wherein each party also generates a first and second hash values and exchanges the first hash values for comparison. However, Menezes discloses that party A sends its

generated first hash value to party B before party B generates its own first and second hash values. The prior art, taken either singly or in combination, fails to anticipate or fairly suggest the limitations of applicant's independent claim, in such a manner that a rejection under 35 U.S.C 102 or 103 would be proper. The claimed invention is therefore considered to be in condition for allowance as being novel and nonobvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

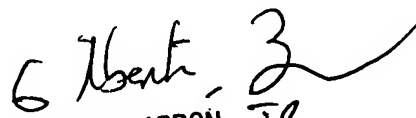
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MD/
Minh Dinh
Examiner
Art Unit 2132

10/05/07


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100